Новые возможности МОШЕННИКОВ

Новые технологии влекут за собой новые возможности злоумышленников, столкнувшись с которыми наши законопослушные граждане не знают, как в таких случаях поступать и предоставления ими любой малозначимой, на их взгляд информации, позволяет злоумышленникам совершить в отношении последних преступление.

Только за первые дни 2021 года Горецким районным отделом Следственного комитета Республики Беларусь возбуждено 6 уголовных дел по признакам состава, предусмотренного ч.2 ст. 212 (Хищение путем использования компьютерной техника) УК Республики Беларусь из которых 4 уголовных дел возбуждены по фактам хищения денежных средств, совершенные посредствам удаленного доступа к мобильным устройствам потерпевших.

В данном случае речь идет о все том же известным **ВИШИНГЕ**, то есть о методе мошенничества, суть которого заключается в телефонной коммуникации, введении в заблуждение, претворяясь сотрудником банка, покупателем и так далее, и выманивании под разными предлогами у держателя платежной карты конфиденциальной информации или стимулировании к совершению определенных действий со своим банковским счетом и/или платежной картой.

Однако если в вышеуказанной описанной ситуации злоумышленники завладевают сведениями (реквизитами) банковской платежной картой, то в новом способе хищения денежных средств у граждан, в ходе телефонного разговора, последних уверяют о необходимости установки в мобильном телефоне, через магазин приложений «Play Маркет» различных программ удаленного доступа, таких как «TeamViewer» или «AnyDesk», после установки которых злоумышленники имеют возможность осуществлять доступ к установленным в мобильном устройстве потерпевших, мобильными приложениями, такими как к примеру: «Интернет-банкинг», «М-банкинг» и другие, используя которые совершают хищение денежных средств со счетов граждан без уточнения реквизитов банковских карт.

Чтобы обезопасить граждан от противоправных действий мошенников, Горецкий районный отдел Следственного комитета Республики Беларусь призывает граждан к здравому смыслу при беседе со злоумышленниками, а также бдительности.

Если Вам позвонили из «банка» с просьбой предоставить реквизиты банковской карты, так как в настоящее время совершается хищение денежных средств с Вашего счета, ПОМНИТЕ:

- Не отвечайте на неизвестные номера входящих вызовов, которые поступают через мессенджер «Viber»;
- В случае если Вы вступили в разговор, в ходе которого звонящее лицо Вам, представилось «работником банка», просто прекращайте разговор, положив трубку;
- Никому, в том числе лицам, представившимся «работниками банка», не сообщайте реквизиты своей банковской карты (номер карты, имя и отчество,

срок действия, cvc-код, указанный с обратной стороны карты), в том числе идентификационный номера паспорта;

- Ни при каких обстоятельствах не устанавливайте в своем мобильном телефоне никаких приложений, которые необходимы якобы для работы звонившим «работникам банка»;
- В случае, если Вы ответили на входящий вызов и Вам стало известно, что с Вашего счета осуществляется списание, перевод или хищение денег, **прекратите разговор** и незамедлительно перезвоните в службу сервиса Ваше банка, абонентский номер которого указан на обратной стороне принадлежащей Вам банковской карты.

Валерий Дрюков,
старший следователь следственного отделения
Горецкого районного отдела
Следственного комитета Республики Беларусь